

SYSTEM AND METHOD FOR IDENTIFYING A MACRO VIRUS FAMILY USING A MACRO VIRUS DEFINITIONS DATABASE

Abstract

A system and method for identifying a macro virus family using a macro virus definitions database is described. A macro virus definitions database is maintained and includes a set of indices and associated macro virus definition data files. One or more of the macro virus definition data files are referenced by the associated index. Each macro virus definition data file defines macro virus attributes for known macro viruses. The sets of the indices and the macro virus definition data files are organized according to macro virus families. One or more strings stored in a suspect file are compared to the macro virus attributes defined in the one or more macro virus definition data files for each macro virus family in the macro virus definitions database. The macro virus family to which the suspect file belongs is determined from the indices for each of the macro virus definition data files at least partially containing the suspect file.